



OCR

Oxford Cambridge and RSA

An OCR endorsed
teaching and learning tool

OCR A Level

Computer Science

H446 – Paper 1



Network security and threats

Unit 5
Networks and web
technologies



PG ONLINE

Objectives

- Discuss network security and threats
- Discuss use of firewalls, proxies and encryption
- Discuss worms, Trojans and viruses and the vulnerabilities that they exploit

Starter

- A file is being transferred from Chile to India
 - What risks are involved in sending confidential information within the file?



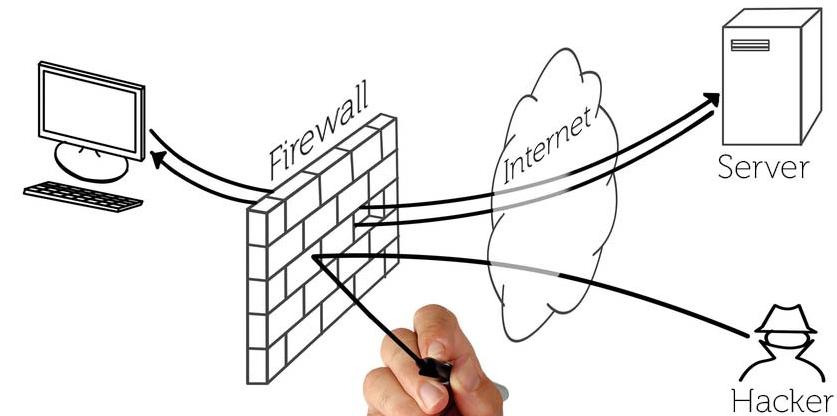
Castle security

- How can you get in or out of a castle?
 - What can you do to stop people entering or leaving?



Firewall

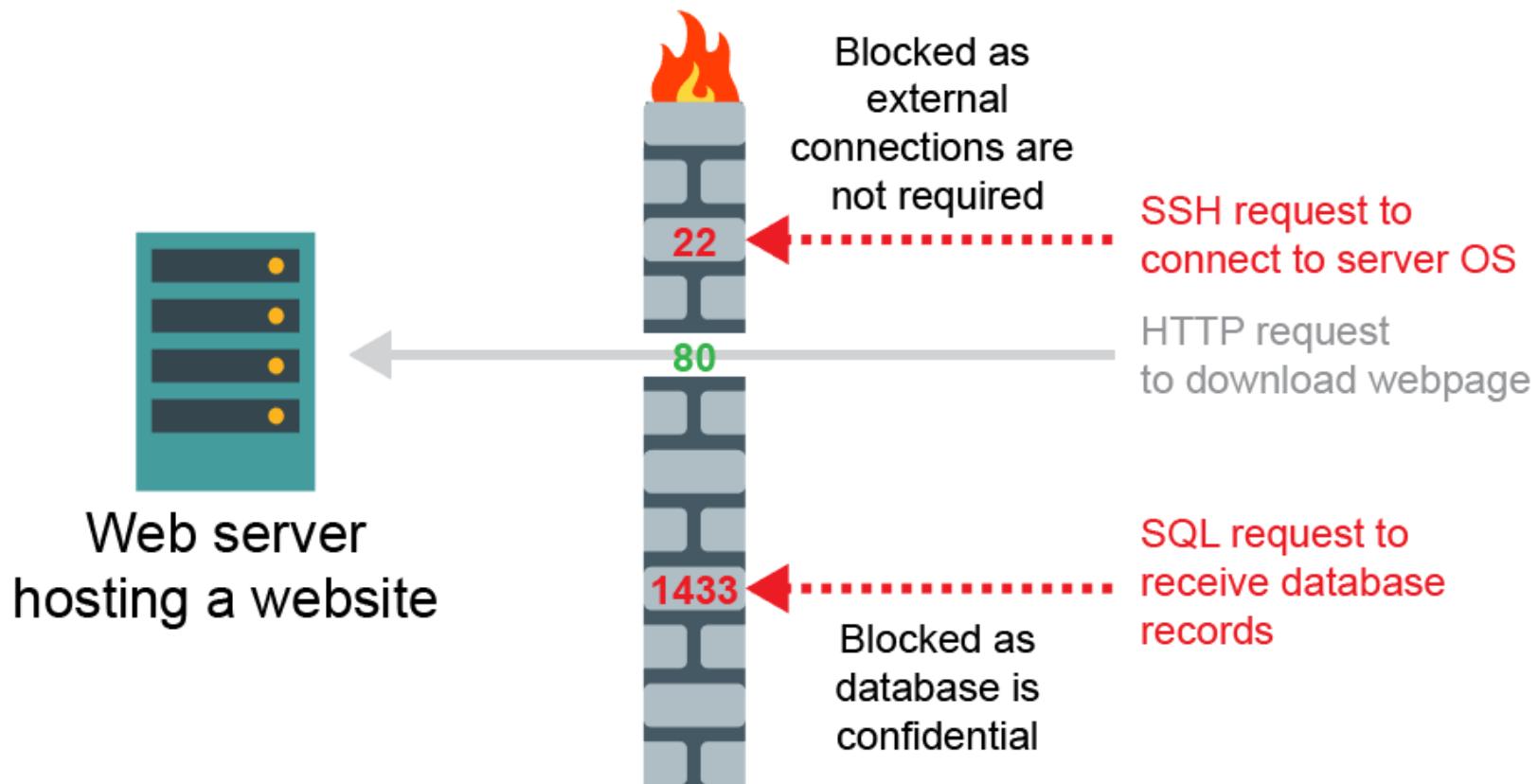
- The entrance to a network can be protected in the same way
 - A firewall is either software or hardware that controls access to and from a network
 - Numbered doors called **ports** are opened so that only certain traffic is allowed to pass through



Packet filtering

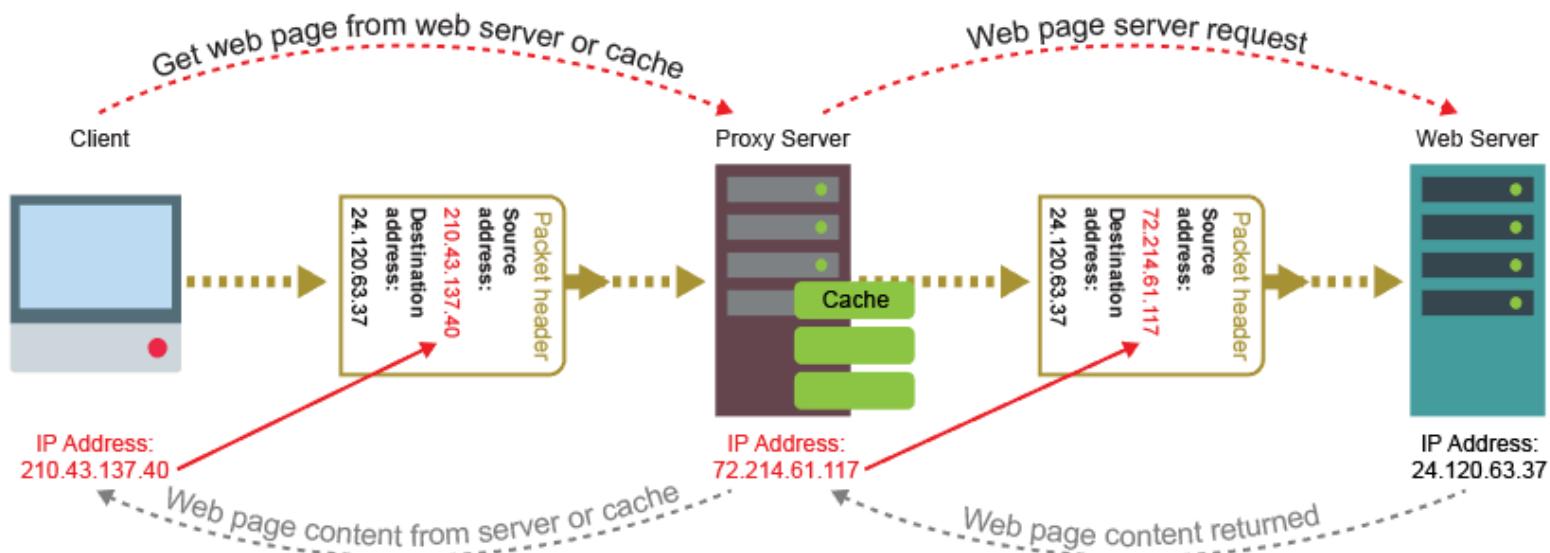
- Packets of data are inspected by the firewall to check which port they are attempting to access
- Different network protocols use different port numbers for example, HTTP traffic, used to transfer web page data, uses port 80 or 8080
- If this traffic is to be allowed through, the port must be opened for the duration of the connection, otherwise the firewall will automatically reject it
 - Why are ports not left open by default?

Blocking communications



Proxy servers

- ‘Proxy’ means ‘*on behalf of*’
 - A proxy server makes a web request on behalf of your own computer, hiding the true request IP addresses from the recipient



Functions of a proxy server

• A proxy server:

- Enables anonymous surfing
- Can be used to filter undesirable online content
- Logs user data with their requests
- Provides a cache of previously visited sites to speed access
- What happens if the website has been updated since the cached version?

Worksheet 3

- Complete **Task 1**



Encryption

- The act of encoding a plaintext message so that it cannot be deciphered unless you have a numerical key to decrypt it
 - If the message is intercepted it cannot be understood
 - If the key can be intercepted, the encryption process is rendered useless
 - (Encryption is covered in much greater detail in Unit 4)

Malicious software

- Malware annoys users or damages their data
- Worms and viruses self-replicate
- A virus infects (embeds itself in) other programs or data files
- A virus needs a user to help it spread
 - It is commonly found in email attachments with Macros



Worms

- A worm is a standalone program that does not require a user to run it in order for it to spread
 - Worms exploit vulnerabilities in the destination system and spread automatically



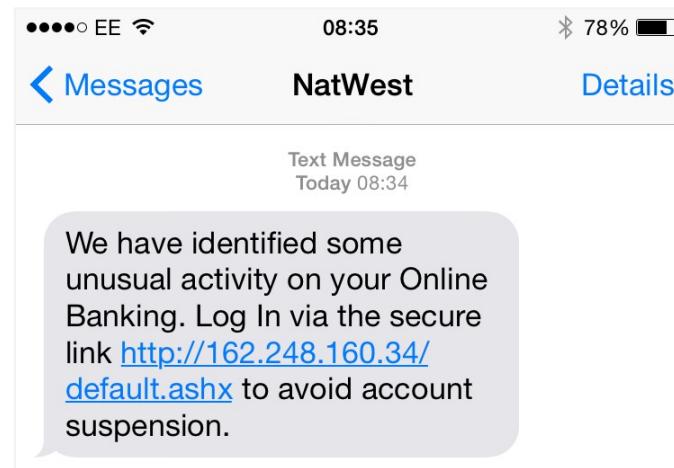
Trojans

- Trojans are malicious software programs that masquerade as innocuous or useful applications
 - They cannot self-replicate
 - Often they serve to open up back doors in your computer to the Internet so that the processing power, Internet bandwidth and data can be exploited remotely



Phishing

- Phishing is using email to manipulate a victim into visiting a fake website and giving away personal information
 - Who is most susceptible to such messages?
 - What are the consequences of clicking on such a link?



Code quality

- Improving code quality, together with monitoring attempts to gain unauthorised access and protection can significantly reduce threats from malware
- Measures include:
 - Guarding against buffer overflow attack
 - Guarding against SQL injection attack
 - Use of strong passwords for login credentials
 - Two-factor authentication
 - Use of access rights (file system permissions)

Buffer overflow

- Buffer overflow occurs when a program accidentally writes data to a location too small to handle it
 - As a result the overflowed **data** (written to location #3 below) may end up in a neighbouring **instruction** space
 - Malware can ~~control~~ **use** and manipulate overflow data  **DATA** **DATA** **DATA** **DATA** **INST** **INST** **INST** **INST**



SQL injection

- A malicious user can enter SQL commands via online database forms to change the processing
 - Imagine the following SQL for a banking web form below:



"S
t> **Find your account details:**
Enter your Customer ID: **21104710; DROP TABLE Accounts;**

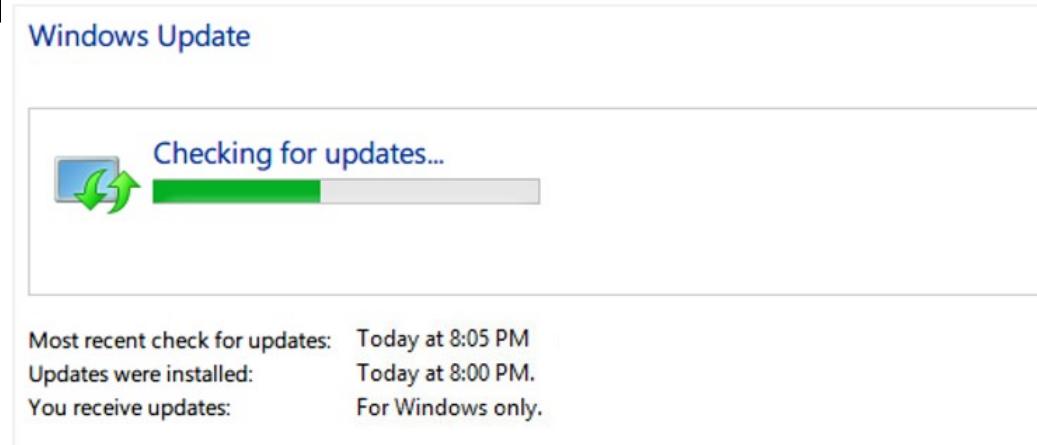
- This will produce the following SQL to display the correct account details, then delete the bank's entire accounts data

Monitoring

- Monitoring can protect against the threat of hacking, which can introduce malware
- These can be used to protect against the threat of malware and hacking
 - Packet sniffers
 - User access logs

Prevention

- Up-to-date patches to the operating system and application programs reduce vulnerabilities in the system
- Up-to-date anti-malware (“anti-virus”) software can prevent the spread of infection



Worksheet 3

- Complete **Tasks 2 - 4**



Copyright

© 2016 PG Online Limited

The contents of this unit are protected by copyright.

This unit and all the worksheets, PowerPoint presentations, teaching guides and other associated files distributed with it are supplied to you by PG Online Limited under licence and may be used and copied by you only in accordance with the terms of the licence. Except as expressly permitted by the licence, no part of the materials distributed with this unit may be used, reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic or otherwise, without the prior written permission of PG Online Limited.

Licence agreement

This is a legal agreement between you, the end user, and PG Online Limited. This unit and all the worksheets, PowerPoint presentations, teaching guides and other associated files distributed with it is licensed, not sold, to you by PG Online Limited for use under the terms of the licence.

The materials distributed with this unit may be freely copied and used by members of a single institution on a single site only. You are not permitted to share in any way any of the materials or part of the materials with any third party, including users on another site or individuals who are members of a separate institution. You acknowledge that the materials must remain with you, the licencing institution, and no part of the materials may be transferred to another institution. You also agree not to procure, authorise, encourage, facilitate or enable any third party to reproduce these materials in whole or in part without the prior permission of PG Online Limited.